

DOCKET NO.: 277747US90PCT

10/550216
JC05 Rec'd PCT/PTO 22 SEP 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kei KARASAWA, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP05/06624

INTERNATIONAL FILING DATE: April 4, 2005

FOR: PACKET CRYPTOGRAPHIC PROCESSING PROXY APPARATUS, METHOD THEREFOR AND RECORDING MEDIUM FOR PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

| <u>COUNTRY</u> | <u>APPLICATION NO</u> | <u>DAY/MONTH/YEAR</u> |
|-----------------------|------------------------------|------------------------------|
| Japan | 2004-111347 | 05 April 2004 |
| Japan | 2004-119225 | 14 April 2004 |

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP05/06624. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Masayasu Mori
Attorney of Record
Registration No. 47,301
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 4 月 5 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 1 1 1 3 4 7

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

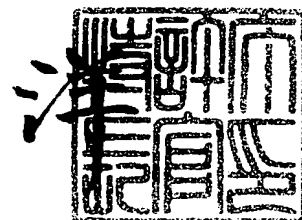
J P 2 0 0 4 - 1 1 1 3 4 7

出 願 人
Applicant(s): 日 本 電 信 電 話 株 式 会 社

2 0 0 5 年 5 月 1 1 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【官 規 則】

付 訂 願

【整理番号】

NTTH157132

【提出日】

平成16年 4月 5日

【あて先】

特許庁長官殿

【国際特許分類】

H04L

【発明者】

【住所又は居所】

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】

唐澤 圭

【発明者】

【住所又は居所】

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】

松浦 克智

【特許出願人】

【識別番号】

000004226

【氏名又は名称】

日本電信電話株式会社

【代理人】

【識別番号】

100066153

【弁理士】

【氏名又は名称】

草野 卓

【選任した代理人】

【識別番号】

100100642

【弁理士】

【氏名又は名称】

稲垣 稔

【手数料の表示】

【予納台帳番号】

002897

【納付金額】

16,000円

【提出物件の目録】

【物件名】

特許請求の範囲 1

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【包括委任状番号】

9806848

【請求項 1】

インターネットと端末装置との間に接続された装置であって、

インターネットに接続された相手装置と前記端末装置との間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路の確立に用いる暗号通信路情報を記憶する暗号通信路情報記憶手段と、

受信されたパケットに対して暗号処理を上記暗号通信路情報記憶手段に記憶されている暗号通信路情報に基づいて行う暗号処理手段と、

を具備するパケット暗号処理代理装置。

【請求項 2】

送信元識別情報、送信先識別情報、パケット通信手順を表すプロトコル情報及び暗号処理をするか否かを示す処理指示情報をフィルタ情報として記憶するフィルタ情報記憶手段と、

このパケット暗号処理装置に受信されたパケット中のフィルタ情報により前記フィルタ情報記憶手段を参照してその処理指示情報に基づき前記受信されたパケットを前記暗号処理手段によって暗号処理をするか否かを判断する暗号処理判断手段を備えることを特徴とする請求項 1 に記載のパケット暗号処理代理装置。

【請求項 3】

前記相手装置から受信されたパケットが正当なものであるか否かを判断する受信パケット判断手段を備えることを特徴とする請求項 1 又は 2 に記載のパケット暗号処理代理装置。

【請求項 4】

前記暗号通信路情報記憶手段は、前記暗号通信路情報中の少なくとも一部が記憶された、着脱可能な耐タンパ性デバイスを備えることを特徴とする請求項 1 ～ 3 のいずれかに記載のパケット暗号処理代理装置。

【請求項 5】

前記相手装置と前記端末装置との間で前記暗号通信路情報を合意するための暗号通信路情報合意手段を備えることを特徴とする請求項 1 ～ 4 のいずれかに記載のパケット暗号処理代理装置。

【請求項 6】

前記暗号通信路情報記憶手段は前記暗号通信路情報中の少なくとも一部が変更可能な記憶媒体を備えることを特徴とする請求項 1 ～ 5 のいずれかに記載のパケット暗号処理代理装置。

【請求項 7】

パケット暗号処理代理装置が、前記端末装置のネットワークインタフェースデバイスに論理的に直接接続されていることを特徴とする請求項 1 ～ 5 のいずれかに記載のパケット暗号処理代理装置。

【請求項 8】

前記インターネットと前記端末装置との間に接続され、IP アドレスを持たないデバイスに前記パケット暗号処理代理装置が実装されていることを特徴とする請求項 1 ～ 5 のいずれかに記載のパケット暗号処理代理装置。

【請求項 9】

前記暗号通信路情報及び前記フィルタ情報の少なくとも一方の一部の情報を前記端末装置から収集する情報収集手段を備えることを特徴とする請求項 2 ～ 8 のいずれかに記載のパケット暗号処理代理装置。

【請求項 10】

インターネットに接続された相手装置と端末装置の間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路の確立に用いる暗号通信路情報を前記相手装置と合意して暗号通信路情報手段に記憶し、

前記暗号通信路情報に基づいて、受信されたパケットに対し暗号処理を行うパケット暗

フ処理方法。

・ 【請求項 11】

前記受信されたバケット中のフィルタ情報により、フィルタ情報記憶手段を参照して前記受信されたバケットに対し、暗号処理をするか、否かを判断し、

前記判断が暗号処理する、であれば前記暗号処理を実行させ、前記判断が暗号処理しない、であれば前記受信されたバケットをそのまま通過又は廃棄することを特徴とする請求項 10 記載のバケット暗号処理方法。

【請求項 12】

請求項 1 ～ 9 のいずれかに記載したバケット暗号処理代理装置としてコンピュータを機能させるためのプログラム。

【発明の名称】 パケット暗号処理代理装置、その方法及びプログラム

【技術分野】

【0001】

この発明は、暗号化、復号化、署名、検証などの暗号処理を行う機能を備えない端末装置とインターネットとの間に接続され、インターネットに接続された相手装置と前記端末装置間のパケット通信における少なくともインターネット上では暗号処理されているパケットに対し、暗号処理を行うパケット暗号処理代理装置、その方法及びプログラムに関するものである。

【背景技術】

【0002】

従来、インターネット等のネットワークを介して暗号通信を行なうための規格として、インターネットの標準化組織である I E T F (Internet Engineering Task Force) により標準化され、フレーム構成、データの暗号化や改ざんチェックなどの規定に準拠した I P S e c (Security Architecture for Internet Protocol) が知られている (例えば、非特許文献 1 参照。)。I P S e c 機能は、端末装置に実装される。その他に、インターネットを利用した仮想的に構築する独自ネットワークであり、標準プロトコルとして I P S e c を規定する V P N (Virtual Private Network) 装置等によって構成されるパケット暗号処理代理装置に実装される。つまり例えばインターネットと L A N (Local Area Network) を接続するゲートウェイ内に I P S e c 機能が設けられ、ゲートウェイが L A N に接続された各端末装置に代ってパケットに対する暗号処理を行う。つまりインターネットに接続された端末装置 (相手装置という) は、L A N に接続された端末装置に対し、データを暗号化しないで通信を行う場合はそのパケットにその L A N の端末装置の I P アドレス等を設定すればよいが、データを暗号化する場合は L A N の端末装置の I P アドレス等を設定し、これとデータを含むパケットを生成し、そのパケット全体に対して所定の暗号化を行い、その暗号化されたパケットに、パケット暗号処理代理装置を兼ねるゲートウェイの I P アドレスなどを設定したパケットを生成し、そのパケットを送信する。このパケットを受信したゲートウェイはそのパケットを復号化し、復号されたパケットを、そのヘッダが示す I P アドレスに基づき L A N の端末に送信する。従ってこの場合のゲートウェイはパケット暗号処理代理装置を兼ねているといえる (第 1 従来技術という)。

【0003】

このようなパケット暗号処理代理装置としては、例えば、アクセスが制限された閉鎖型ネットワークに接続され、閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置 (後の説明では相手装置と対応するもの) との暗号通信を閉鎖型ネットワークに接続された端末装置に代行して行うものがある (例えば、特許文献 1 参照、第 2 従来技術という)。

この特許文献 1 に示す従来のパケット暗号処理代理装置を説明する。図 5 に示すように閉鎖型ネットワークであるホームネットワーク 104 に接続された家庭内ノード 122 と、開放型ネットワークであるインターネット 102 に接続された外部ノード 106 との間で、インターネット 102 とホームネットワーク 104 間に介在されたホームゲートウェイ 108 を介して暗号通信を行う。家庭内ノード (この例では電子レンジ) 122 は、暗号化と復号化の処理を行うために十分なデータ処理性能を備えていない。よってホームネットワーク 104 にパケット暗号処理代理装置として暗号代行家庭内サーバ 120 がホームネットワーク 104 に接続され、家庭内ノード 122 と外部ノード 106 と暗号化通信を行うためのデータ暗号化と復号化の処理を、家庭内サーバ 120 が家庭内ノード 122 に代わって行う。外部ノード 106 が暗号通信の起動を行う場合には外部ノード 106 は、インターネット 102、ホームゲートウェイ 108、ホームネットワーク 104 を経由して暗号通信要求パケットを、家庭内ノードの電子レンジ 122 に送る (S21)。この暗号通信要求パケット内のデータは、外部ノード 106 が家庭内ノードである電子レンジ 122 と暗号通信を確立するために必要なデータであり、電子レンジ 122 に問い合わせ

るノードである。電子レンジ１２２は、このように暗号通信要求パケットを受信したならば、外部ノード１０６に対して、逆の経路で暗号通信承諾パケットを送信する（Ｓ２２）。この暗号通信承諾パケット内のデータには暗号通信を承諾すると共に同じホームネットワーク１０４に接続された家庭内サーバ１２０のネットワークアドレスが含まれている。

【０００４】

暗号通信承諾パケットを受信した外部ノード１０６は、指定された暗号通信代行サーバである家庭内サーバ１２０に対して、インターネット１０２、ホームゲートウェイ１０８、ホームネットワーク１０４を経由して、暗号通信代行要求パケットを送信する（Ｓ２３）。暗号通信代行要求パケットを受信した家庭内サーバ１２０は、暗号通信代行承諾パケットを、その外部ノード１０６に送信する（Ｓ２４）。これによって外部ノード１０６は、家庭内ノード１２２との暗号通信を代行することを確認する。外部ノード１０６は、家庭内サーバ１２０が、家庭内ノード１２２との暗号通信を代行して行うことを確認した後、或いは、これらの確認の全部又は一部を省略して、予め定められた所定の手順に従って暗号化されたデータパケットを家庭内サーバ１２０に送信する（Ｓ２５）。所定の手順に従って暗号化されたデータパケットを受信した家庭内サーバ１２０は、その受信したデータパケットを復号化し、ホームネットワーク１０４を経由して、本来の通信相手であるべき家庭内ノード１２２（電子レンジ）にその復号化されたデータパケットを送信する（Ｓ２６）。これによって、家庭内ノード１２２（電子レンジ）は、高度な暗号化、復号化のための処理能力をもたなくても、本来の目的である外部ノード１０６との暗号通信を実現することができる。

【非特許文献１】RFC (Request for Comments) 2401

【特許文献１】特開２００３－３０４２２７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

第１従来技術ではインターネットに接続された装置は、LANの端末装置に対して、暗号化することなくパケットを送信する場合は、単にそのLANの端末装置のIPアドレスなどを設定すればよいが、暗号化してパケットを送信する場合は、前記暗号化しない場合のパケットを暗号化し、その暗号化されたパケットをデータとし、これに対してゲートウェイ（パケット暗号処理代理装置）のIPアドレスなどを設定してパケットを送信する必要がある。つまり暗号化されないパケットの終端はLANの端末装置であり、暗号化パケットの終端はゲートウェイである。このように暗号通信を行う場合はゲートウェイのIPアドレスなども設定する必要があり、同一端末装置に対する通信にそのIPアドレスなどの他にゲートウェイのIPアドレスなどを設定するという繁雑さがあった。

【０００６】

第２従来技術では、暗号化パケットの終端がパケット暗号処理代理装置にあたる家庭内サーバ１２０であり、パケットの送信先の終端が端末装置（電子レンジ）１２２であるため、家庭内サーバ１２０を導入した場合には、インターネットに接続された相手装置は暗号通信にするか否かによりIPアドレス等の設定情報を変更する必要があり、第１従来技術と同様に通信相手（相手装置を操作する人）に設定の手間をかけてしまうといった問題があった。また、前述したようなこの第２従来技術では、暗号通信を行うにはまず電子レンジ１２２に対し暗号通信要求を行って代行サーバの指定を受け、改めてサーバ１２０に対し暗号通信代行要求とその承諾を受けて暗号化パケットを送るという多くの手間がかかるという問題もあった。

【０００７】

この発明は、これらの問題を解決するためになされたものであり、通信相手に設定の手間をかけずに、暗号処理機能が実装されていない端末装置に対して暗号処理を代行することができるパケット暗号処理代理装置、その方法及びプログラムを提供することを目的とするものである。

【課題を解決するための手段】

【００００】

この発明によるバケット暗号処理代理装置は、インターネットと端末装置との間に接続され、暗号通信路情報記憶手段及び暗号処理手段を備え、暗号通信路情報記憶手段には、インターネットに接続された相手装置と上記端末装置との間のバケット通信における少なくともインターネット上のバケット通信に対し、暗号通信路確立に用いる暗号通信路情報が記憶され、暗号処理手段では受信されたバケットに対して、暗号通信路情報記憶手段に記憶されている暗号通信路情報に基づいて暗号処理が行われる。

【発明の効果】

【０００９】

この発明のバケット暗号処理装置によれば、ネットワーク端末装置との間に接続されているから、例えばインターネットに接続された相手装置では暗号処理機能を備えない端末装置のＩＰアドレスなどを設定すれば暗号処理されたバケットに対する暗号処理、例えば復号が行われるため、つまり相手装置はトランスモードを探ることができ、端末装置のＩＰアドレスなどとバケット暗号処理代理装置ＩＰアドレスなどとの設定を行う必要がなく、相手装置の利用者に設定の手間をかけない、また端末装置との通信により暗号処理代行サーバのＩＰアドレスなどの入手の後、そのサーバのＩＰアドレスなどを設定して暗号処理されたバケットを暗号処理代行サーバへ送信するなどの煩雑さもない。

【発明を実施するための最良の形態】

【００１０】

以下、この発明の実施形態について、図面を参照して説明する。

図１は、この発明の一実施形態に係るバケット暗号処理代理装置１を含むシステムの構成例を示すブロック図である。以下の説明ではバケット暗号処理をＩＰＳｅｃに基づいて行う場合を例とし、暗号処理として暗号化処理及び復号化処理を例とする。

バケット暗号処理代理装置１はインターネット２に接続され、インターネット２には相手装置３が接続される。バケット暗号処理代理装置１はパーソナルコンピュータや通信機能を備え、家庭内電気製品等の端末装置５にＬＡＮ４を介して接続されている。相手装置３には、ＩＰＳｅｃ機能が実装されていても、されていなくてもよいが、端末装置５にはＩＰＳｅｃ機能が実装されていない。この実施形態においては、相手装置３は、ＩＰＳｅｃ機能が実装されたものとする。つまりこの実施形態ではバケット暗号処理代理装置１はインターネットごとＬＡＮ４とを接続するゲートウェイと兼用されている。

【００１１】

バケット暗号処理代理装置１は、ネットワーク２を介して接続された相手装置３等の装置と通信を行うネットワークインタフェース１０と、インターネット２上で安全な通信路を確立するために必要な暗号通信路情報を相手装置３と端末装置５との間で合意するための暗号通信路情報合意手段１１、合意された暗号通信路情報を記憶する暗号通信路情報記憶手段１２、ＩＰＳｅｃに準拠して暗号化されたバケットを復号化する復号化手段１３、端末装置５などとの通信を行う端末インタフェース１４とを備える。

暗号通信路情報はＩＰＳｅｃに準拠したものであり、本来の通信に先立ち相手装置３と端末装置５との間で双方が通信可能な手順の確認のネゴシエーション、つまり合意が暗号通信路情報合意手段１１により行われ、その結果の暗号通信路情報が暗号通信路情報記憶手段１２に記憶される。

【００１２】

暗号通信路情報記憶手段１２は、例えば不揮発性の記憶媒体によって構成される。暗号通信路情報（以下、単に「ＳＡ（Security Association）情報」という）は非特許文献１で規定されたものであり、（１）ＳＡ情報を識別するための３２ビットの整数値で割り当てられて各バケット中に挿入され、バケット内の通信内容を示す識別番号（Security Parameter Index、ＳＰＩ）、（２）通信データ完全性を保証して転送し、またその検証を行うためのプロトコルであるＡＨ（Authentication Header）および通信データを秘匿して転送し、またその秘匿解除するためのプロトコルであるＥＳＰ（Encapsulating Security Payload）の何れかのプロトコルの情報を表すプロトコル情報、（３）暗号化や認証でそ

れて利用される暗号化アルゴリズムや暗号鍵情報、(4)受信したパケットを11パケットを含めて暗号化して受信先へ転送するモードであるトンネルモードおよび、受信したパケット中のデータを暗号化しそれにIPヘッダを付加し、受信先に送るモードであるトランスポートモードの何れかのモードを表すモード情報、(5)IPアドレス及びポート番号よりなる識別子、および(6)SA情報を変化させる時期などを示すSA情報の生存時間等が含まれる。なお、ポート番号はインターネットで標準化されたサービスプロトコルに割り当てられた番号である。この実施形態ではモード情報はトランスポートモードとされるが、例えばIPSec機能を備えない端末装置の他にIPSec機能を備えた端末装置が混在しているネットワークとインターネットとの間にこの発明装置1が設けられる場合はモード情報としてはトンネルモードとされたりトランスポートモードにされたりする。またこの実施形態ではプロトコル情報としてはESPが用いられるが、データが改ざんできないようにするAHプロトコル、具体的には例えばデジタル署名及びその検証のプロトコルを用いてもよい。

【0013】

SA情報の各パラメータは、IKE(Internet Key Exchange)等の鍵交換プロトコルによって通信相手との間で合意されるものであり、暗号通信路情報合意手段11は、端末装置5に代わってSA情報の各パラメータを相手装置3と合意し、合意したパラメータが反映されたSA情報を暗号通信路情報記憶手段12に格納する。

復号化手段13は、暗号通信路情報記憶手段12に記憶されたSA情報に含まれる暗号アルゴリズムや暗号鍵情報に基づいて、相手装置3によってIPSecに準拠して暗号化されて端末装置5に向けて送信されたパケットをパケットの送信元と送信先を変えずに復号化する。

【0014】

更に、この実施形態ではパケット暗号処理代理装置1は、送信元識別情報、送信先識別情報、およびパケット伝送プロトコル情報に対応して、パケットの処理を表す指示情報をフィルタ情報として記憶するフィルタ情報記憶手段15と、相手装置3によって送信されたパケットを復号化手段13によって復号化するか否かをフィルタ情報に基づいて判断する復号化判断手段16を備えている。

復号化判断手段16は、フィルタ情報記憶手段15にあらかじめ記憶されているフィルタ情報を参照し、相手装置3によって端末装置5に向けて送信されたパケットを復号化するか、端末装置5にそのまま端末インタフェース14を介して送信するか、パケットを廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。

【0015】

図2は、フィルタ情報の例を示した表である。図2において、1列目は、パケットの送信元を識別するための送信元識別情報中の送信元のIPアドレスを表し、2列目はパケットの送信先を識別するための送信先識別情報を構成する送信先のIPアドレス、3列目はパケットを伝送するための通信手順を表すプロトコル情報、4列目は送信元識別情報中の送信元のポート番号、5列目は送信先識別情報中の送信先のポート番号、および6列目はパケットをどのように処理するかを表す処理指示情報を表している。従って、前述したように復号化判断手段16は、受信したパケット中の処理指示情報以外のフィルタ情報によりフィルタ情報記憶手段15にあらかじめ記憶されているフィルタ情報を参照し、その処理指示情報に応じて端末装置5に向けて送信されたパケットを復号化するか、そのまま端末インタフェース14を介して送信するか、この例では更に廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。

【0016】

図2中の1行目は、IPアドレスがIPv4によって書かれており、送信元のIPアドレスが10.0.0.1/32、送信先のIPアドレスが10.0.0.*/*24(上位24ビットが10.0.0.、下位8ビットが0~24)および、プロトコル情報が信頼性を保証したコネクション形プロトコルであるtcp(Transmission Control Protocol)の場合には、送信元ポート番号及び送信先ポート番号が何番であっても(any)、処理指示情報は相手装置3によって送

に与えられたパケットを暗号処理する。

また、2行目は、IPアドレスがIPv6によって書かれており、送信元のIPアドレスが2001::1、送信先のIPアドレスが2001::2、プロトコル情報がパケットの紛失を許容するコネクションレス形プロトコルであるudp (User datagram protocol)、および、送信元のポート番号と送信先のポート番号とが137の場合には、処理指示情報は相手装置3によって送信されたパケットを端末装置5にそのまま端末インタフェース14を介してバイパス送信する。

【0017】

また、3行目は、送信元のIPアドレスが2001::1/128、送信先のIPアドレスが2001::2/128、プロトコル情報がIP端末同士をコントロールするプロトコルであるicmp (Internet Control Message Protocol)、および、送信元のポート番号が135の場合には、処理指示情報は相手装置3によって送信されたパケットを廃棄する。なおこれらは例示であって、その識別情報やプロトコル情報と処理指示情報との間に関連はない。

なお、復号化判断手段16は受信したパケット中のフィルタ情報に基づきフィルタ情報記憶手段15を参照したらその処理指示情報は復号化であったが、その受信されたパケットのヘッダ情報を参照し、その暗号化されているか否かを示すパケットが暗号化されているか否かを表わす情報によれば、そのパケットがIPSecに準拠して暗号化されていないと判断されると、このパケットを廃棄するあるいは端末装置5へそのままバイパスしてもよい。

【0018】

この実施形態では、パケット暗号処理代理装置1は復号化判断手段16が復号化と判断した場合に、復号化処理に先立って相手装置3によって送信されたパケットが正当なものであるか否かを判断する受信パケット判断手段17がさらに備えられている。受信パケット判断手段17によるパケットの正当性の判断は、IPSecに準拠して暗号化されたパケットに含まれる完全性チェック値やIPSecの規定されているパケットに付随しているシーケンス番号等に基づいて行われる。なお、完全性チェック値 (Integrity Check Value、ICV) は、認証アルゴリズムによって決定されるアルゴリズムによって算出される。受信パケットが復号化と判断された後、そのパケットがそのヘッダ情報を参照して暗号化されているか否かを判断することは受信パケット判断手段17で行ってもよい。

【0019】

更にこの実施形態では、パケット暗号処理代理装置1は、暗号通信路情報記憶手段12に記憶されたSA情報に基づいて、端末装置5によって送信されたパケットをIPSecに準拠して暗号化する暗号化手段18と、フィルタ情報記憶手段15に記憶されたフィルタ情報に基づいて、端末装置5によって送信されたパケットを暗号化手段18によって暗号化するか否かを判断する暗号化判断手段19とが備えられている。

暗号化手段18は、暗号通信路情報記憶手段12に記憶されたSA情報に含まれる暗号アルゴリズムや暗号鍵情報に基づいて、端末装置5によって相手装置3に向けて送信されたパケットをIPSecに準拠してパケットの送信元と送信先を変えずに暗号化する。

【0020】

暗号化判断手段19は、端末装置5から受信したパケット中のフィルタ情報 (処理指示情報を除く) によりフィルタ情報記憶手段15に記憶されたフィルタ情報を参照し、端末装置5によって送信されたパケットを暗号化して送信するか、相手装置3にそのままネットワークインタフェース10を介して送信するか、パケットを廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。なお、暗号化判断手段19によって参照されるフィルタ情報は、図2を用いて説明した復号化判断手段16によって参照されるフィルタ情報と同様であるため、説明を省略する。ただ同一フィルタ情報であっても相手装置5から端末装置3へのパケットと、端末装置3から相手装置5へのパケットとにより前者は復号化するが、後者は暗号化しないなど処理指示情報が異なる場合もあり、個々に決められている。

- ・ フィルタ情報を参照する暗号化判断手段 1 9 を設けることによって、バケット暗号処理代理装置 1 は、複数の端末装置が接続された場合に、あらかじめ予定（許可）されていない不正な端末装置を相手装置と接続するのを防ぐことができ、同様にあらかじめ予定（許可）されていない不正な相手装置 3 との間で暗号通信が行われることを防ぐことができる。

以下に、バケット暗号処理代理装置 1 の動作を説明する。なお、以下に説明するバケット暗号処理代理装置 1 の各動作において、暗号通信路情報合意手段 1 1 によって合意されたパラメータが反映された S A 情報が、暗号通信路情報記憶手段 1 2 に既に記憶されているものとする。

【 0 0 2 2 】

図 3 は、バケット暗号処理代理装置 1 の相手装置 3 からのバケット受信動作を示すフローチャートである。バケット暗号処理代理装置 1 の相手装置 3 からのバケット受信動作は、ネットワーク 2 を介して相手装置 3 によって端末装置 5 に向けて送信されたバケットがネットワークインタフェース 1 0 によって受信されたときにバケット暗号処理代理装置 1 は始まる。

まず、復号化判断手段 1 6 が、ネットワークインタフェース 1 0 によって受信したバケット中のフィルタ情報によりフィルタ情報記憶手段 1 5 に記憶されたフィルタ情報を参照し、受信されたバケットを復号化するか否かが判断され（S 1）、復号化すると判断されないと端末装置 5 にそのまま端末インタフェース 1 4 を介して送信するか否かが判断され（S 2）、そのまま送信しないと判断されるとその受信バケットは復号化判断手段 1 6 により廃棄される（S 4）。

【 0 0 2 3 】

ステップ S 1 でバケットを復号化すると判断された場合には、ネットワークインタフェース 1 0 によって受信されたバケットが正当なものであるか否かが受信バケット判断手段 1 7 によって判断される（S 3）。ネットワークインタフェース 1 0 によって受信されたバケットが正当なものでないと判断された場合には、ネットワークインタフェース 1 0 によって受信されたバケットが受信バケット判断手段 1 7 によって廃棄される（S 4）。

一方、ステップ S 4 でネットワークインタフェース 1 0 によって受信されたバケットが正当なものであると判断された場合には、ネットワークインタフェース 1 0 によって受信されたバケットが暗号通信路情報記憶手段 1 2 に記憶された S A 情報に基づき復号化手段 1 3 によって復号化され（S 5）、復号化されたバケットが端末インタフェース 1 4 および L A N 4 を介して端末装置 5 に送信される（S 6）。

【 0 0 2 4 】

ステップ S 2 で、ネットワークインタフェース 1 0 によって受信されたバケットを端末装置 5 にそのまま端末インタフェース 1 4 を介して送信すると復号化判断手段 1 6 によって判断された場合には、ネットワークインタフェース 1 0 によって受信されたバケットが端末インタフェース 1 4 および L A N 4 を介して端末装置 5 に送信される（S 6）。

図 4 は、バケット暗号処理代理装置 1 の端末装置 5 からのバケット受信動作を示すフローチャートである。この場合のバケット暗号処理代理装置 1 の動作は、L A N 4 を介して端末装置 5 によって相手装置 3 に向けて送信されたバケットが端末インタフェース 1 4 によって受信されたときに開始する。

【 0 0 2 5 】

まず、暗号化判断手段 1 9 により、端末インタフェース 1 4 で受信されたバケットのフィルタ情報に基づきフィルタ情報記憶手段 1 5 に記憶されたフィルタ情報を参照して、その受信されたバケットを暗号化するか否かが判断され（S 1 1）、暗号化しないと判断されると、相手装置 3 にそのままネットワークインタフェース 1 0 を介して送信するか否かが判断され（S 1 2）、そのまま送信しないと判断された場合、バケットを廃棄すると判断された場合には、その受信されたバケットが暗号化判断手段 1 9 によって廃棄される（S 1 5）。

【 0 0 2 0 】

ステップ S 1 1 でパケットを暗号化すると判断された場合には、端末インタフェース 1 4 によって受信されたパケットが、暗号通信路情報記憶手段 1 2 に記憶された S A 情報に基づき暗号化手段 1 8 によって I P S e c に準拠して暗号化され (S 1 3)、その暗号化されたパケットがネットワークインタフェース 1 0 およびインターネット 2 を介して相手装置 3 に送信される (S 1 4)。

ステップ S 1 2 で端末インタフェース 1 4 によって受信されたパケットを相手装置 3 にそのままネットワークインタフェース 1 0 を介して送信すると暗号化判断手段 1 9 によって判断された場合 (S 1 2) には、端末インタフェース 1 4 によって受信されたパケットがネットワークインタフェース 1 0 およびインターネット 2 を介して相手装置 3 に送信される (S 1 4)。

【 0 0 2 7 】

以上で説明した、パケット暗号処理代理装置 1 の各構成要素は、上記で説明した動作をさせるように記述されたプログラムをプロセッサに実行させるようにしてもよい。すなわち、復号化手段 1 3、復号化判断手段 1 6、受信パケット判断手段 1 7、暗号化手段 1 8、および暗号化判断手段 1 9 は、上記プログラムを実行するコンピュータによって構成するようにしてもよい。この場合、コンピュータ内にこのパケット暗号処理代理プログラムを C D - R O M、磁気ディスク、半導体記憶装置などの記録媒体からインストール又は通信回線を通じてダウンロードしてそのプログラムをコンピュータに実行させればよい。

【 0 0 2 8 】

また、暗号通信路情報記憶手段 1 2 およびフィルタ情報記憶手段 1 5 のうち少なくとも一方は、記憶した情報の少なくとも一部を、例えば暗号鍵情報、利用者名などを予定された (許された) 以外の利用者が変更できないように、 I C カード、 U S B (Universal Serial Bus) キー、 S D (Secure Digital) メモリカードなどの、耐タンパ性のある着脱可能なデバイスによって構成してもよい。

一方、暗号通信路情報記憶手段 1 2 およびフィルタ情報記憶手段 1 5 のうち少なくとも一方は、インターネット 2 を介して認証された利用者であるならば、記憶した情報の少なくとも一部を変更できるようにしてもよい。つまり、例えば相手装置 3 と端末装置 5 との通信相手をダイナミックに変更し、これに伴い I P アドレスを変更する。この場合は、パケット暗号処理代理装置 1 には、 I P アドレスを割り当て、その I P アドレスを用いてパケット暗号処理代理装置 1 とパケット通信を行って例えばそのフィルタ情報記憶手段 1 5 に記憶するフィルタ情報に対する変更を行う。

【 0 0 2 9 】

上述においてはパケット暗号処理代理装置をゲートウェイに設けたが、このパケット暗号処理装置は I P 機能をもたないものであり、前記実施形態では受信したパケットを暗号処理するか否かの判断をして、暗号処理をする場合はパケット送信元及び送信先を変更することなく暗号処理を行って、そのパケットを送信先へ転送し、暗号処理を行わない場合はそのままパケットを送信先へ転送するものである。つまり暗号処理を行う場合と行わない場合とにより I P アドレスを変更したり、2 つの I P アドレスを用いたりする必要がなく、従来のゲートウェイに設けられている、 I P 機能をもつパケット暗号処理代理装置とは異なる。

【 0 0 3 0 】

この発明のパケット暗号処理代理装置としてはフィルタ情報に基づく処理を行わなくてもよく、つまり単に暗号処理を行うだけでもよく、その場合も、暗号処理機能をもたない端末装置と相手装置とのパケット暗号通信の際に、相手装置はパケット送信先として端末装置の I P アドレスを付加すればよく、暗号処理代理装置の I P アドレスを用いる必要はない。

この発明のパケット暗号処理代理装置はインターネット 2 と端末装置 5 との間に接続されていればよく、例えば図 1 に破線で示すように L A N 4 と各端末装置 5 との間に接続してよい。この場合は端末装置 5 には L A N との接続カード、つまり I P 機能をもつ接続カ

ードが表名とされているが、ついでにLAN接続カードにバケット暗号処理代理装置1を接続してもよい。

【0031】

IPSec機能はIP機能の一部として実装される。従って従来においてはゲートウェイのIP機能にIPSec機能が組み込まれ、あるいは端末装置のIP機能にIPSec機能が組み込まれていた。しかしこの発明の実施形態のバケット暗号処理代理装置1ではIP機能に組み込まれることなく、最も簡単なものは暗号通信路情報記憶手段と暗号処理手段だけの機能をもっていればよく、つまりIP機能と切り離され、送信先及び送信元を変更することなく単に暗号処理をして通過させるものである。従って単に端末装置のIPアドレスをバケットに設定すればよく端末装置のIPアドレスとバケット暗号処理代理装置のIPアドレスとの両アドレスをバケットに設定したり、IPアドレスの使い分けをする必要がなく、また暗号処理代行サーバのIPアドレスを入手した後にバケット暗号処理を行う繁雑さもない。

【0032】

このようにこの発明の実施形態のバケット暗号処理代理装置1はそのIPSec機能はIP機能に組み込まれるものでないから、インターネット2と端末装置5との間であればいずれの箇所に挿入してもよい。例えば図1中に破線で示すようにLAN4と端末装置5との間に挿入してもよい。この場合は端末装置5に搭載されている、インターネットを介する通信機能、つまりIP機能が有線LANカードや無線LANカードなどのネットワークインタフェースデバイスにこの実施形態のバケット暗号処理代理装置を実装してもよく、この発明装置1は端末装置5に論理的に直接接続されてもよい。

【0033】

同様に図1中に破線で示すようにLAN4に2ポートイーサネット（登録商標）ブリッジ6を介して端末装置5が接続されている場合のようにIPアドレスを持たないネットワーク間接続機器にこの実施形態のバケット暗号処理代理装置1を実装してもよい。つまりインターネットと端末装置との間に接続されているIPアドレスを持たないデバイスにこの発明装置1を実装してもよい。更に図1中に破線で示すように例えば家庭内のパーソナルコンピュータなどのIP機能をもつ端末装置5が公衆通信網7を介してインターネット2に接続されている場合に、その端末装置5と公衆通信網7との間にこの実施形態のバケット暗号処理装置1を挿入してもよい。つまり端末装置5はインターネット2と論理的に直接接続されている場合でもこの実施形態を適用することができる。

【0034】

この発明において暗号処理とは前述したように、データを秘匿する、つまり暗号化する処理、その秘匿データとの秘匿を解除する、つまり復号化する処理、電子署名などデータの完全性を保証する処理、その署名の検証などの完全性を確認する処理のいずれかである。相手装置3から受信したバケットに対してのみこの発明を適用してもよく、逆に端末装置5から受信したバケットに対してのみこの発明を適用してもよい。例えば前者の場合は図1中の暗号化手段18及び暗号化判断手段19は省略され、端末インタフェース14に受信されたバケットはそのままネットワークインタフェース10に送られ、後者の場合は復号化判断手段16、受信バケット判断手段17、復号化手段13が省略され、ネットワークインタフェース10に受信されたバケットはそのまま端末インタフェース14に送られる。

【0035】

図1に示す構成中の受信バケット判断手段17は省略してもよい。つまり受信バケットの正当性の判断は端末装置5のIP機能により判断させてもよい。しかし受信バケット判断手段17を設ければ不必要なバケットに対し無駄な復号化処理がなされない効果がある。

フィルタ情報記憶手段15及び復号化判断手段16を省略してもよい。この場合は端末装置5に対し送信するバケットは全て暗号処理されたバケットにする必要がある。しかしこれら手段15及び16を設ければ、バケットのデータに要求される事項などに応じて、

- ・ 暗号処理するがしらないがをばいかりてパケットを暗号化直前に返送することができ、暗号処理を施さなくてもよいパケットに対して暗号処理しないで済み、相手装置3の処理が簡単になる。フィルタ情報記憶手段15及び暗号化判断手段19も同様に省略することができる。しかしこれら手段を設ければ同様に不必要に暗号化処理を行わないで済み、この装置1の処理負荷が軽くなる。

【0036】

なお暗号処理手段と暗号通信路情報記憶手段のみを設けたパケット暗号処理代理装置1を端末装置5の直前に設ける場合においても、利用者名や装置製造番号など外部に秘匿しておきたいデータに対し暗号化されるために有効である。

パケット暗号処理代理装置1に、ARP(Address Resolution Protocol、アドレス解決プロトコル)やNDP(Neighbor Discovery Protocol、近隣発見プロトコル)などの情報収集プロトコルや、UPnP(Universal Plug and Play)などの相互接続機能をもつ情報収集手段20を設け、パケット暗号処理代理装置1がこれに接続されている端末装置5のIPアドレスやサービス等の機器情報を収集し、収集した機器情報に基づいてポート番号やプロトコルの種別などのIPアドレスを生成して、また端末装置5が外された場合にパケット暗号処理代理装置1か暗号通信路情報およびフィルタ情報のうち少なくとも一方を生成する際の利用者による入力を支援するようにしてもよい。フィルタ情報記憶手段中の対応フィルタ情報を削除するようにし、フィルタ情報記憶手段中の無駄なフィルタ情報を減らすことによりフィルタ情報の参照が効率的に行われるようにする。このようにパケット暗号処理代理装置1に、図2に示したような項目の入力としての利用者入力の支援や情報管理を行わせるようにしてもよい。

【0037】

例えば、空調機、照明器具、洗濯機、電話機、電子レンジ、テレビジョン受像機、パーソナルコンピュータなどの家庭内電気機器、事務用電気機器などその他あらゆる電気機器であって、IP機能を備えるものである。LAN4は無線LAN、有線LANでもよく、用途的に云えばホームネットワーク、企業内ネットワーク、学校内ネットワーク、地域ネットワーク、病院内ネットワークなどである。

上述でパケットに対する暗号処理をIPSecにより準拠して行っただが、他の規格SSL(Secure Sockets Layer)やTLS(Transport Layer Security)などにより暗号処理を行ってもよい。

【図面の簡単な説明】

【0038】

【図1】この発明の一実施形態によるパケット暗号処理代理装置を含むシステム構成例を示すブロック図。

【図2】図1中のフィルタ情報記憶手段15中に記憶されているフィルタ情報の例を示す図。

【図3】この発明の一実施形態によるパケット暗号処理代理方法における相手装置から受信したパケットに対する処理手順の例を示すフローチャート。

【図4】この発明の一実施形態によるパケット暗号処理代理方法における端末装置から受信したパケットに対する処理手順の例を示すフローチャート。

【図5】従来のパケット暗号処理代行サーバを含むシステム及び代行暗号処理の通信手順を示す図。

【図1】

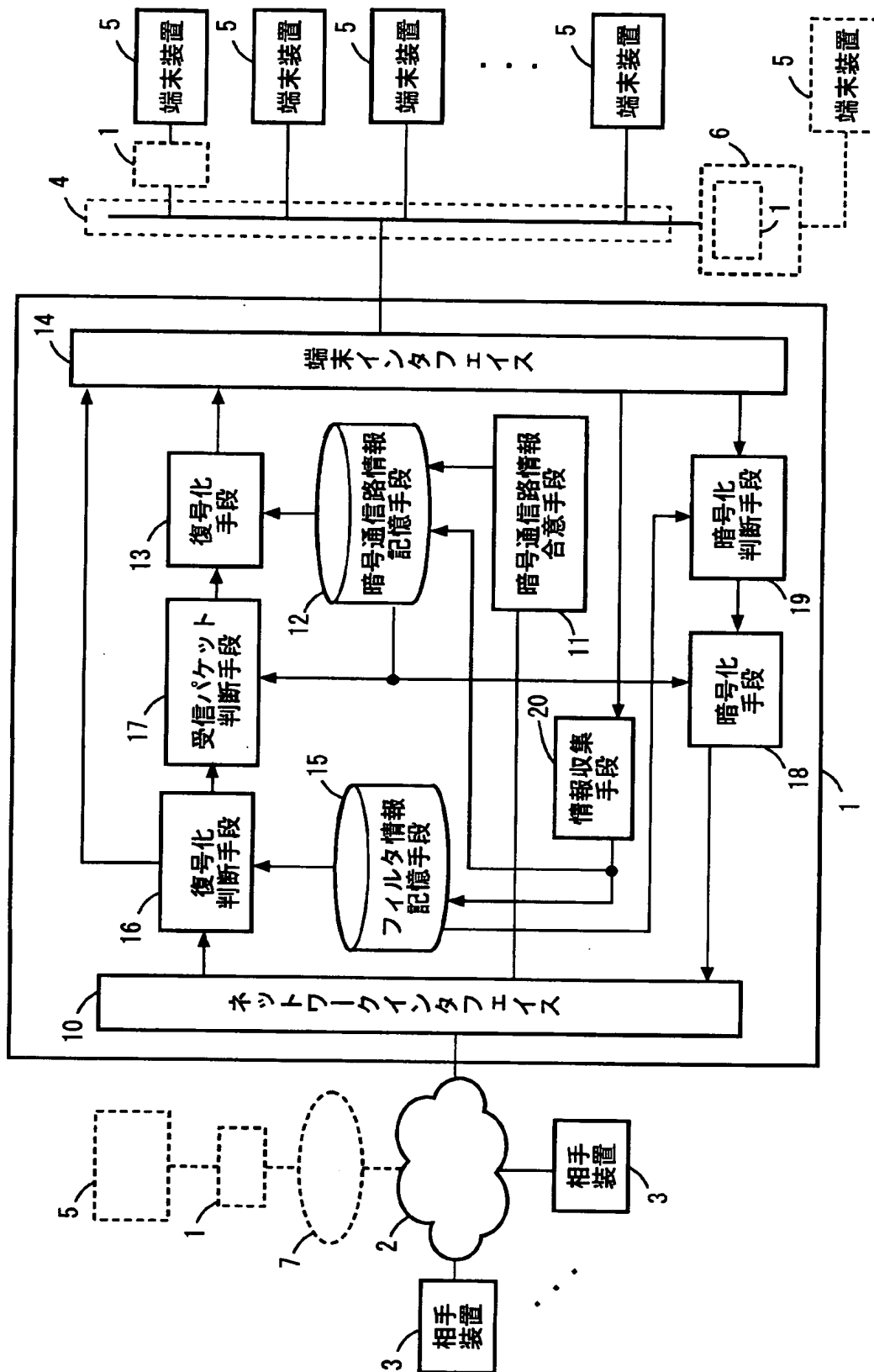


図1

| 送信元IPアドレス | 送信先IPアドレス | プロトコル | 送信元ポート番号 | 送信先ポート番号 | 処理指示 |
|-------------|---------------|-------|----------|----------|------|
| 10.0.0.1/32 | 10.0.0.*/*/24 | tcp | any | any | 暗号処理 |
| 2001::1 | 2001::2 | udp | 137 | 137 | バイパス |
| 2001::1/128 | 2001::2/128 | icmp | 135 | N/A | 廃棄 |

図2

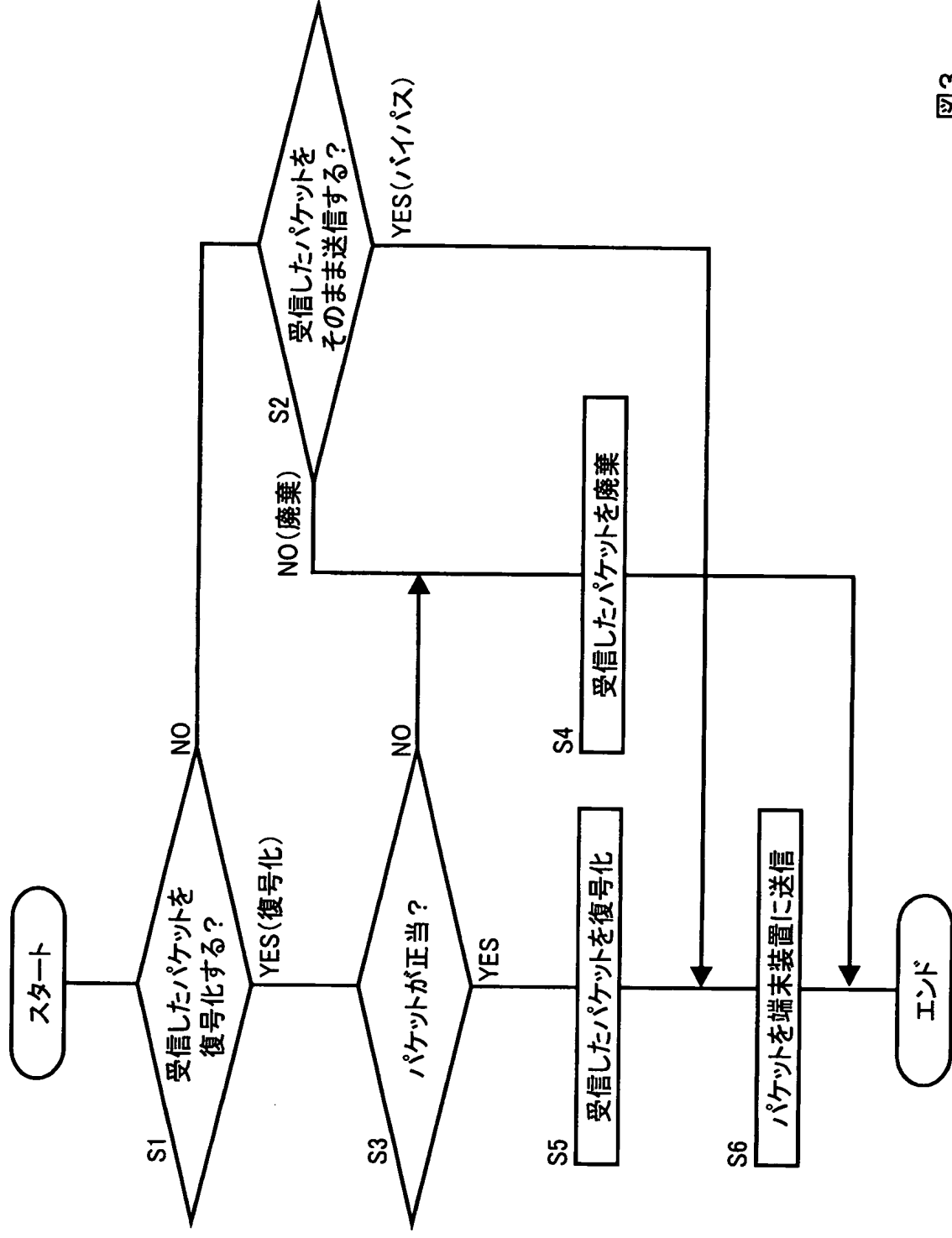


図3

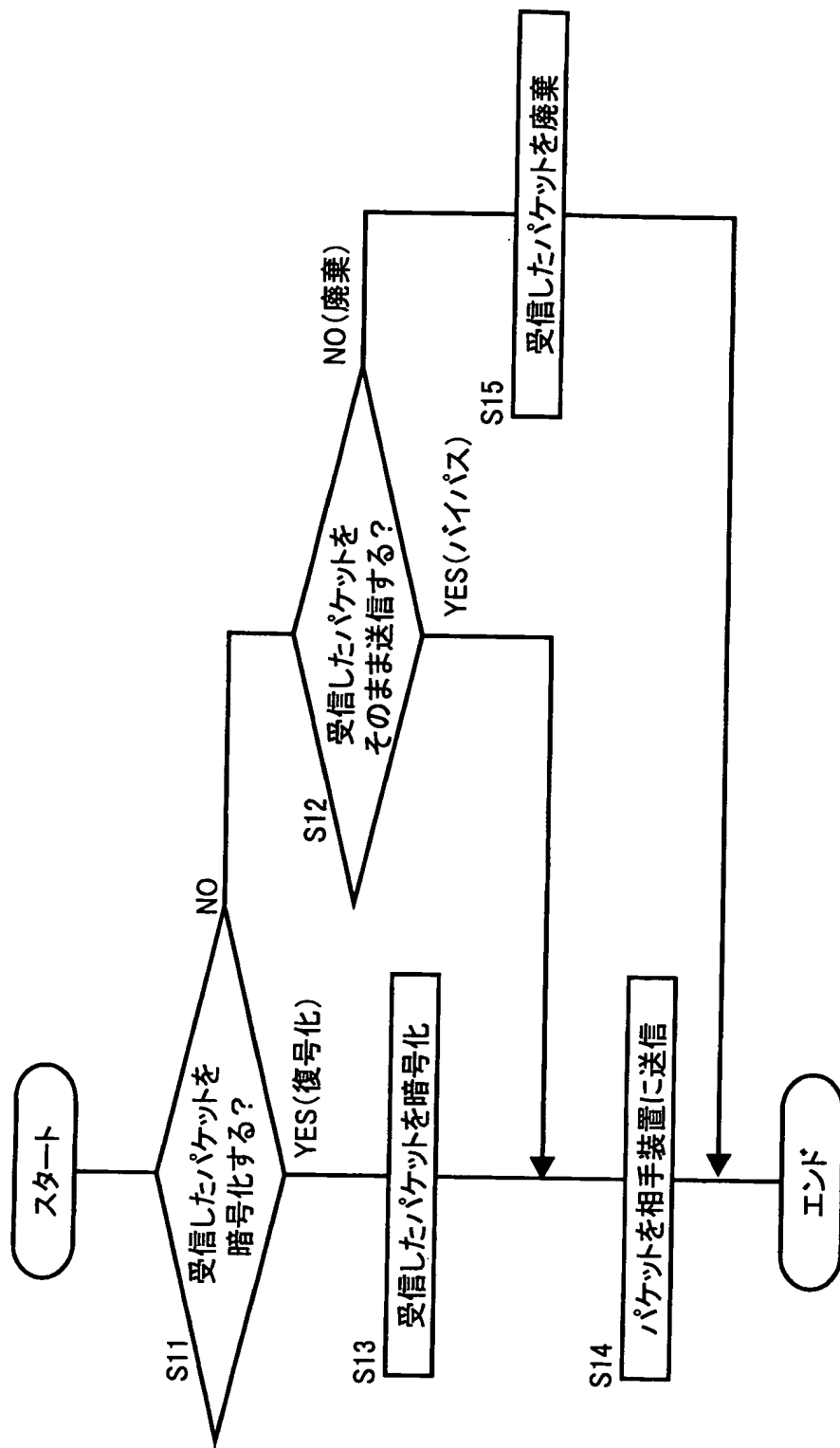
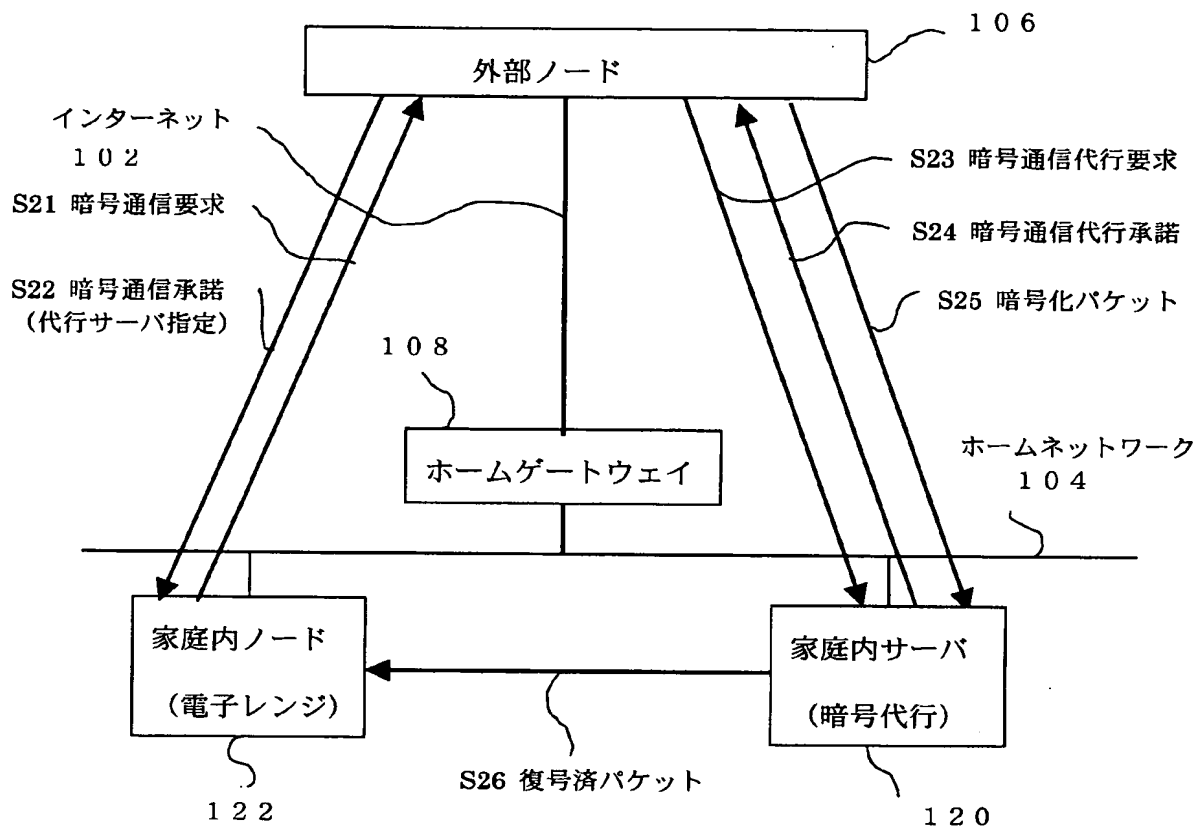


図4

図 5



【要 約】

【課題】 I P S e c 機能がない端末に対し、I P S e c 処理の代理をし、通信相手に設定の手間をかけない。

【解決手段】 インターネット 2 に接続された相手装置 3 からパケットが受信されると、そのパケット中の送信元及び送信先の I P アドレス・ポート番号、プロトコルにより、フィルタ情報記憶手段 1 5 を参照して、復号化するかバイパスするかを手段 1 6 で判断し、復号化と判断されると、記憶手段 1 2 から、装置 3 と I P S e c 機能をもたない端末 5 とで予め合意された暗号通信路情報に基づいて受信パケットを復号化して端末 5 へ送る。暗号通信路情報は装置 3 と 5 の間に I P S e c に準拠したパケット通信路を確立するために用い、識別番号、暗号化処理か署名処理かのプロトコル情報、暗号アルゴリズムや鍵情報、I P アドレス・ポート番号などである。相手はトランスポートモードを使用できる。

【選択図】 図 1

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006624

International filing date: 04 April 2005 (04.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-111347
Filing date: 05 April 2004 (05.04.2004)

Date of receipt at the International Bureau: 26 May 2005 (26.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse